Crypto Consult (PTY) LTD

FSP 55052 | REG: 2024/392954/07
389 Victoria Street, Waterkloof, Pretoria, 0181
L: +27 12 460 1330 | M:+27 68 607 8728

CRYPTO CONSULT (PTY) LTD

POPI Policy

2026

Date of issue/update	Created: 16/02/2026 Last reviewed and/or updated: 16/02/2026	Version	1.0
Policy owner	Gideon Frylinck		
Approved by	Gideon Frylinck	16/02/2026	

Crypto Consult (PTY) LTD

FSP 55052 | REG: 2024/392954/07
389 Victoria Street, Waterkloof, Pretoria, 0181
L: +27 12 460 1330 | M:+27 68 607 8728

CRYPTO CONSULT
THE NEXT ERA OF INVESTING

PERSONAL INFORMATION:

This Policy outlines how Crypto Consult (Pty) Ltd ("the FSP") collects, processes, stores, shares, and protects personal information in compliance with the Protection of Personal Information Act, No. 4 of 2013 ("POPIA").

This policy applies to all employees, representatives, contractors, and third-party service providers of the FSP who process personal information on behalf of the FSP. It also applies to all data subjects whose personal information is collected and processed by the FSP, including but not limited to clients, employees, and suppliers.

DEFINITIONS:

''**consent**'' means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

''**data subject**'' means the person to whom personal information relates;

''**de-identify**'', in relation to personal information of a data subject, means to delete any information that—

(a) identifies the data subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

"information officer" of, or in relation to, a—

(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
(b) (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

"processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

"responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

PRINCIPLES

The FSP is committed to upholding the 8 conditions for lawful processing of personal information as outlined in POPIA:

1. **Accountability**

   The FSP takes responsibility for ensuring that personal information is processed in accordance with POPIA.

2. **Processing Limitation**

   Personal information is collected directly from the data subject and only processed for legitimate, specific, and lawful purposes.

3. **Purpose Specification**

   Personal information is collected for defined purposes related to financial services, and not further processed in a manner incompatible with those purposes.

4. **Further Processing Limitation**

Any further processing of personal information will be compatible with the original purpose of collection.

5. Information Quality

The FSP will take reasonable steps to ensure that personal information is complete, accurate, and up to date.

6. Openness

The FSP will maintain the documentation of all processing operations and inform data subjects about the collection of their personal information where required.

7. Security Safeguards

Appropriate, reasonable technical and organizational measures will be implemented to safeguard personal information against loss, damage, unauthorised access, or unlawful processing.

8. Data Subject Participation

Data subjects have the right to access, correct, or delete their personal information within reasonable timeframes and processes.

TYPES OF PERSONAL INFORMATION COLLECTED

Depending on the nature of the services provided, the FSP may collect and process the following types of information:

- Identity number, name, surname
- Contact details (email, phone number, address)
- Financial information (bank account number)
- Employment details
- Tax and statutory information
- Records of correspondence
- Information related to risk profiles, investment preferences, or insurance needs

PURPOSE OF COLLECTION

The FSP collects and processes personal information to:

- Provide financial services in accordance with FAIS and other applicable laws
- Conduct client onboarding and due diligence (e.g. FICA and KYC requirements)
- Process applications for financial products or services

- Manage and administer client relationships
- Conduct legal, compliance, and risk management procedures
- Communicate with clients and stakeholders
- Fulfil contractual and legal obligations
- Conduct market research and customer satisfaction surveys
- Maintain accurate audit and record-keeping
- Perform credit assessments and credit management

HOW IS THE INFORMATION COLLECTED

1. **Directly from the client**
   The FSP ordinarily collects personal information during the client onboarding process, via electronic communication (e.g. email), telephone, or in-person interactions. The specific information collected will depend on the nature of the service, product offering, and the FSP's legal and regulatory requirements.

2. **From third-party sources**

Additional personal information may be obtained from third parties, including:

- Independent financial advisers, discretionary investment managers, or authorised agents acting on behalf of the client
- Verification service providers for compliance with statutory obligations, such as anti-money laundering laws and general background checks

SHARING AND TRANSFER OF INFORMATION

The FSP is committed to protecting personal information and will not sell, rent, or trade such information to any third party. However, personal information may be shared in the following circumstances:

- With authorised employees and representatives of the FSP
- With product providers, insurers, or third-party service providers necessary to fulfil the agreed service
- With other third parties where consent has been provided or where required by law
- Upon request by regulatory authorities (e.g. Financial Sector Conduct Authority, Prudential Authority, Financial Intelligence Centre) exercising their statutory powers
- Pursuant to a valid court order

International Transfers:

Where the client holds offshore investments, personal information may be transferred to and processed in jurisdictions with equivalent data protection standards, including:

- The European Economic Area (EEA) – subject to the EU General Data Protection Regulation (GDPR)
- Guernsey – subject to the Data Protection (Bailiwick of Guernsey) Law, 2017
- Bermuda – subject to the Personal Information Protection Act, 2016 (PIPA)
- Botswana – subject to the Data Protection Act, 2024 (DPA)

Where personal information is transferred outside of these jurisdictions, the FSP will apply appropriate safeguards, including contractual obligations, to ensure compliance with both South African and applicable foreign data protection laws.

STORAGE

Personal information is stored securely and retained only for as long as necessary to achieve the purpose for which it was collected or as otherwise required by law.

After a client relationship has ended, the FSP may retain personal information for up to five years, for the following reasons:

- To comply with legal and regulatory retention obligations
- For prudent record-keeping in relation to services rendered

Where information is subject to ongoing legal proceedings or other statutory requirements, the FSP may retain such information beyond the five-year period.

KEEPING INFORMATION TO-DATE

The FSP is committed to ensuring that all personal information is accurate, complete, and current. To this end:

- Reasonable steps will be taken to verify personal information at the time of collection and periodically thereafter
- Clients and data subjects are encouraged to notify the FSP of any changes to their personal information, including contact details, employment, or marital status
- Where personal information is found to be inaccurate or outdated, it will be promptly updated upon receipt of the correct details or a valid request from the data subject
- The FSP may periodically request confirmation or updates of personal information to meet regulatory and operational obligations

SECURITY

The FSP takes all reasonable precautions to ensure the confidentiality, integrity, and availability of personal information in its possession. Security measures are regularly reviewed and updated in line with legislative and technological developments.

Current safeguards include:

- Firewalls and anti-virus software
- Access control and password protection
- Data encryption for sensitive information
- Secure physical and digital document storage
- Regular staff training on data privacy and protection

DATA SUBJECT RIGHTS

In terms of POPIA, data subjects have the following rights:

- To be informed about the collection and use of their personal information
- To access the personal information the FSP holds about them
- To request correction, deletion, or destruction of personal information
- To object to the processing of their personal information in certain circumstances
- To lodge a complaint with the Information Regulator of South Africa

INFORMATION OFFICER

Any questions relating to the FSPs privacy policy or the treatment of an individual's personal data may be addressed to the contact details below:

Information officer:
- Gideon Frylinck

Telephone number:
- +27 12 460 1330

Postal address:
- 254 Church Avenue
  Lynnwood
  Pretoria, Gauteng 0081

Physical address:
- 254 Church Avenue
  Lynnwood
  Pretoria, Gauteng 0081

Email address:
- info@cryptoconsult.co.za

Website:
- https://www.cryptoconsult.co.za/